UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
Houston Division

HAYDEN D. PARKHILL,
***on behalf of himself and all others similarly situated*,**

Plaintiff,

v. **Case No. _____**

EQUIFAX, INC.
SERVE: Prentice-Hall Corporation System
211 E. 7th Street
Suite 620
Austin, TX 78701

EQUIFAX INFORMATION SERVICES, LLC,
SERVE: Corporation Service Company
211 E. 7th Street, Suite 620
Austin, TX 78701

Defendant.

CLASS ACTION COMPLAINT

COMES NOW Plaintiff, Hayden D. Parkhill, on behalf of himself and all other Texas consumers similarly situated, by counsel, seek judgment against Defendant Equifax Inc. and Equifax Information Services, LLC ("EIS"), (collectively, "Equifax") and states as follows:

Preliminary Statement

1. This is an action for actual damages, costs and attorneys' fees brought pursuant to common-law negligence. Defendant negligently allowed the fraudulent procurement of the critical private information of Plaintiff and Class Members' consumer report files, and failed to disclose the fact of such procurement from Plaintiff.

2. Defendants operate together as a unified consumer reporting agency ("CRA") to prepare and furnish consumer reports for credit and other purposes. Equifax's databases contain a treasure trove of valuable information about nearly every American adult—account numbers and payment histories, Social Security numbers, names and aliases, birthdates, addresses, employment histories, and the like—that Equifax collects and sells to businesses that extend credit, loan money, sell insurance, and grant employment, among numerous other activities.

3. Defendants obtain the largest portion of its vast store of data independently and without consumers' consent or knowledge. Put differently, consumers rarely turn data over to Equifax knowingly and willingly—most of the data Equifax possesses it obtained from sources other than the consumers themselves.

4. In May of 2017, and likely earlier, unknown individuals electronically accessed Equifax's databases without Equifax's knowledge, gaining access to information about approximately 143,000,000 Americans.[1] Ironically, the identity thieves entered Equifax's systems through the Internet portal it uses to receive consumer disputes of identity theft and other credit inaccuracies,[2] and then accessed collateral database information from there, including Defendants' core consumer contact database, "ACIS."[3]

5. Defendants have disclosed generally that the fraudulent users procured consumers' names, Social Security numbers, birthdates, addresses, and driver's license numbers.[4] The breach

[1] *See* https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do. All information regarding the data breach in these opening Paragraphs comes from this FTC publication.
[2] Equifax had created that portal as a means to fully automate its "reinvestigations" of consumer disputes and – in theory – avoid the expense of having live human beings oversee that process and obligation.
[3] "ACIS" is Equifax's acronym for its "Automated Consumer Interview System".
[4] https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

lasted for months and, although Equifax knew about the security vulnerability in May, and the breach itself in July at the latest, it sat on this information until September 8, 2017.

6. Plaintiff and Class Members include Texas consumers regarding whom Equifax possessed information protected by federal Fair Credit Reporting Act, which was thereafter unlawfully procured by identity thieves between May and July 2017. In addition, to protect themselves after Equifax's data breach, Plaintiff and Class Members contacted Equifax's competing consumer reporting agencies ("CRAs"), Experian and TransUnion, and requested a "security freeze" under Texas Business and Commerce Code Section 20.034. As Texas law permits, Experian and TransUnion charge consumers $10 for implementing the freeze. TEX. BUS. & COMM. CODE ANN. § 20.04 (West 2007).

7. Plaintiff and Class Members incurred this expense due to Equifax's negligence and, naturally, their fear that their identities will be stolen, bank accounts emptied, and lifelong credit histories ruined.

8. Plaintiff therefore asserts a negligence claim for himself and all other Texas consumers following Equifax's data breach. Equifax possessed significant, important financial data about them but failed to exercise the standard of care as should a reasonable entity with such "grave responsibilities" that come along with the right to store and sell such information. 15 U.S.C. § 1681(a)(4). Because of that failure, Equifax permitted unauthorized access to Plaintiff's and Class Members' personal information, which in turn caused them to suffer not only actual harm caused by the stress of not being able to know what was accessed and how it will be used by the perpetrators of the breach, the risk of harm that their identities will be stolen, accounts improperly accessed, or credit injured, among other potential harms, and the otherwise needless outlay of cash to other CRAs to place security freezes on their credit files.

Jurisdiction And Venue

9. The jurisdiction of this Court is conferred by 28 U.S.C. § 1332 and 28 U.S.C. § 1367. Defendant Equifax is a corporation headquartered in Atlanta, Georgia, and Plaintiff and all consumers embraced by the Class definition below reside in Texas. There is more than $5 million dollars, exclusive of interest and costs, at stake in this case.

10. Defendant Equifax is subject to personal jurisdiction in the Southern District of Texas, Houston Division, by virtue of the business it conducts in the Division. Venue is proper in this jurisdiction.

Parties

11. Plaintiff is a natural person and a "consumer" as defined by the FCRA.

12. Plaintiff has reason to believe, based upon public reports of the Data Breach, its scale, and upon information provided by Equifax via its website, that his personal identifying information ("PII") was taken during the Data Breach.

13. Plaintiff is a resident of Katy, Texas. Following Equifax's public disclosure of the breach on September 7, 2017, Plaintiff accessed Equifax's website which stated to him that he "may" be a victim of the Data Breach. Plaintiff has devoted significant time to monitoring his accounts in response to the Data Breach. To protect himself as best he would be able, Plaintiff contacted Experian and TransUnion on September 14, 2017, and instituted a security freeze for his files with both CRAs. Plaintiff paid the required fee of $10 to each CRA to institute the freeze. Plaintiff was never alerted or advised by Equifax that his consumer report information had been procured as a result of the Data Breach.

14. Defendant Equifax, Inc. is the parent Equifax Information Services, LLC. In prior litigation, it has taken the position that it is not itself a "consumer reporting agency" governed by

the FCRA. *See* 15 U.S.C. § 1681a(f) ("The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.")

15. But of course, Equifax, Inc. *is* a consumer reporting agency. For purposes of the FCRA, Equifax, Inc. has held itself out repeatedly to consumers, regulators and the public generally as the actual operating entity. The branding, labels and disclosures on the Defendants' consumer website is dominated by "Equifax, Inc." titling. Defendants have held Equifax, Inc. out as the operating and responsible entity.

16. Defendant Equifax Information Services, LLC is a foreign limited liability company transacting business in Texas and maintains a registered office in Austin, Texas. At all times relevant to this action, Defendant Equifax was a "consumer reporting agency" as defined by the Fair Credit Reporting Act, 15 U.S.C. § 1681a–x, and the Texas Business and Commerce Code, TEX. BUS. & COMM. CODE ANN. § 20.01(5).

17. The FCRA, through a rule mandated at § 1681x, expressly prohibits "a consumer reporting agency from circumventing or evading treatment as a consumer reporting agency" by means of corporate reorganization or structuring.

18. Equifax, Inc. and its subsidiary – whether or not they observe state law corporate formalities – have eliminated nearly all lines between the different business entities in the collection, maintenance, sharing and furnishing of consumer reporting information. Equifax, Inc., and entities such as EIS regularly share FCRA restricted information with sibling entities to market

and profit from the sale of consumer identity theft prevention products, including the blurring of legal lines between providing file information under the FCRA versus for private sale to the consumer. Equifax subsidiary TALX Corporation operates as Equifax Workforce Solutions, and with control of acquired-entity eThority and both provides and obtains FCRA-governed consumer information to and from other Equifax entities. Equifax entity Anakam, Inc. integrates Equifax consumer data for sale of its fraud detection and verification products, largely now under the Equifax brand. And, by last example Equifax Mortgage Services operates as a separate entity focused on the mortgage services industry, but also freely shares and uses otherwise FCRA protected data.

19. Further, throughout this breach and post-exposure conduct, the Defendants have operated and acted as one entity and CRA.

20. Here, Equifax, Inc. has used EIS as a dependent and integrated division rather than a separate legal entity. The business operations are fully coordinated and shared. Resources are cross-applied without full and complete cost and profit centers. Management decisions at EIS is made by and through management at Equifax, Inc. And the entities largely hold themselves out as a single uniform business.

21. For purposes of the claims here, these facts are especially meaningful. Data security was shared and the negligence here was directly that of management officials at Equifax, Inc. In fact, it was Equifax. Inc.'s Chief Security Officer Susan Mauldin and Chief Information Officer David Webb who Defendants have fired as a result of the events alleged herein, rather than employees of the subsidiary entities. Equifax, Inc.'s president has directed all matters related to these events. And Equifax, Inc.'s General Counsel was and has remained the Chief Legal Officer and compliance official for all Equifax entities.

22. To remain separate and distinct for the purposes of liability in this action, Defendants must operate as separate and legally as well as operationally distinct entities. Here, for matters and functions alleged and relevant herein, EIS was merely an alter ego of Equifax, Inc. For purposes of how consumer data was handled, warehoused, used and sold, the corporate lines were disregarded in practice. EIS was a mere instrumentality for the transaction of the corporate consumer credit business. The Defendants shared full unity of interest and ownership such that the separate personalities of the corporation and subsidiaries no longer existed.

23. Further, recognition of the technical corporate formalities in this case would cause an irremediable injustice and permit Equifax, Inc. – the entity whose management ran, caused and permitted the events alleged herein – to defeat justice and to evade tort responsibility. *Heyde v. Xtraman, Inc.,* 199 Ga. App. 303, 306, 404 S.E.2d 607 (1991).

24. Accordingly, for all purposes hereafter, when the Plaintiffs allege "Equifax" as the actor or responsible party, they are alleging the participation and responsibility of all three Defendants collectively.

25. Equifax is regularly engaged in the business of assembling, evaluating, and disbursing information concerning consumers for the purpose of furnishing "investigative consumer reports," as defined in 15 U.S.C. § 168ld and TEX. BUS. & COMM. CODE ANN. § 20.01(5), to third parties.

Facts

Equifax Breached its Duty of Care in Causing and Permitting the Data Breach

26. Equifax's business is information. It gathers, through third-party submissions and by accessing public and other records, information on nearly every American adult. It sells this information to countless businesses so that they may make decisions such as whether to grant

credit, offer employment, loan money, issue insurance, rent housing, and the like. Equifax is strictly governed by the FCRA and state laws, but also holds common-law obligations to secure the information it possesses and protect it from unauthorized dissemination.

27. Equifax is aware that it is held to a heightened duty of care to protect its consumer file information. The text of its governing statute, the FCRA, itself warns Equifax of its "grave responsibilities" to maintain the privacy of consumer data, language that has been often repeated in court decisions in which Equifax was involved. And the Defendants even acknowledge in their 2016 Annual Report that, "We are subject to a number of U.S. and state and foreign laws and regulations relating to consumer privacy, data and financial protection. These regulations are complex, change frequently, have tended to become more stringent over time[.]"

28. The standard duty of care for Equifax was significant. It possessed – for profit and resale – the very private personal identifiers and financial information on nearly every consumer in the nation. In fact, Equifax possesses significantly greater amounts of that information than even the Federal and State governments, which themselves have to purchase reporting products from Equifax to discover such information. The standard for Equifax's maintenance and monitoring of its systems is much greater than an ordinary business.

29. The Gramm–Leach–Bliley Act ("GLBA"), 15 U.S. Code § 6801, and the regulations promulgated thereunder also imposed a duty on Equifax to ensure the security and confidentiality of customer records and information, to protect against hazards including unauthorized access or use, and to notify affected customers as soon as possible of any breach of security.

30. Equifax owed these duties, in particular, to Plaintiffs and Class Members, as persons whose personal identifying information ("PII") and other information was in Equifax's possession.

31. Equifax had a special relationship with the Plaintiffs and Class Members because it was entrusted with their personal information. Equifax's ability to acquire Class Members' PII and other information from them and other entities, created an independent duty of care because it was predicated on the understanding, based on Equifax's own representations, that Equifax would take adequate security precautions.

32. Further, Equifax's trade in the private and critical financial information of consumers poses an abnormally dangerous risk of financial harm to those consumers.

33. EIS is the entity that Equifax uses to warehouse and administer the retail credit information and credit reporting function for U.S. consumers. It gathers the information from third parties it labels "subscribers," referred to as "furnishers" under the FCRA, builds files matching that data to specific consumers and stores it in a database it titles "ACRO."

34. Separately, Equifax maintains the ACIS database which includes all documents created or obtained by Equifax from consumer contacts, such as consumer disputes, requests for a copy of the consumer's own credit file, correspondence sent to the consumer, and substantial amounts of data generated to document and archive each of these contacts. Communications that come in from the Equifax Internet portal that was the conduit for the data breach are maintained in the ACIS system. And Equifax has tried to convince the public generally that its "core database" was not breached. But that distinction is meaningless as entry into the ACIS system provides access to nearly all of the same data – personal identifiers, accounts, etc. – that would be useful

from the ACRO database. And access through ACIS gets a user directly into other data troves containing comparable information.

35. In the modest amount of information that it has released publicly, Equifax admits that its security team first observed suspicious network traffic associated with its U.S. online dispute portal web application no earlier than July 29, 2017 and continuing overnight into July 30, 2017.

36. Equifax cannot state with any certainty when this intrusion began.

37. Equifax has represented that the Data Breach occurred when hackers entered its dispute portal through a vulnerability via something called "Apache Struts." Apache Struts is an open-source application framework that allows applications to run on a web server.

38. At a high level, an application framework can be thought of as "prepackaged" computer code that is specifically designed to allows users to then write their own custom code, add it to the environment, and then allow the prepackaged code portions to run the custom code portions so that in house programmers do not need to reinvent the wheel every time they build an application.

39. Since application frameworks are specifically designed to incorporate other pieces of code that are not part of the package (in this case, Apache Struts), they are particularly vulnerable to attack since the software is designed to and given permission to run code portions that are custom designed by in house programming teams (or in this case, outsiders).

40. The particular vulnerability with Apache Struts that was exploited in this case allowed outsiders to run their custom code packages while they were uploading a file.

41. When this general Apache Struts vulnerability first became public knowledge in early March 2017, it was deemed a "0 day" exploit. This means that hackers became aware of the vulnerability before the developers of the software did.

42. Accordingly, a patch was released on March 7, 2017 and available publicly for download as a "critical patch."

43. The patch was rated with a NIST score of "10" meaning that on a 1–10 scale, this was the most critical type of vulnerability known to the developers.

44. Notwithstanding that the particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017, Equifax failed to successfully apply the "patch" to its systems that would have fixed the problem.

45. Between March 7, 2017 and July 29, 2017, Equifax did not successfully apply the patch, if it even attempted to at all.

46. Equifax admits that the unauthorized accesses to certain files containing personal consumer reporting information occurred between, at least, May 13, 2017 through July 30, 2017. Equifax is also unable to rule out that the problem may have started even earlier during a separate successful and similar hack in March 2017 of its payroll subsidiary TALX (responsible for its "Work Number" payroll information product that Equifax markets to employers and data brokers).

47. The information obtained from TALX, particularly W-2 information stolen just before tax season, was likely a gold mine to those intruders as it allowed them to file false income tax returns.

48. Form W-2 information frequently sells in the range of $40 to $50 per individual between criminals on the internet.

49. Following a review by Mandiant, an outside security company that also investigated the March 2017 TALX breach but somehow still failed to correct this vulnerability, Equifax concluded that personal information relating to 143 million U.S. consumers – primarily names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers were breached, in addition to credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with credit and other personal identifying information for approximately 182,000 U.S. consumers.

50. Since the breach, sources have reported that personal identifying information accessed during the breach, including addresses, social security numbers, dates of birth and driver license numbers for various celebrities and public figures are presently offered for sale on the "Dark Web."

51. The Dark Web is a portion of the internet that is not accessible with traditional web browsers or through conventional search engines, but allows users with the proper system configuration to anonymously browse hidden websites and communicate with each over via highly encrypted messaging protocols.

52. While the Dark Web and its associated "TOR" browser technology is widely used by criminals to traffic in various categories of illicit materials, including drugs, firearms, professional hitman services, child pornography, and now apparently the private financial information of most of the adult population of the United States of America previously maintained by Equifax.

53. On September 20, 2017, Comodo Threat Intelligence Labs reported its findings that the individuals that breached Equifax's system also injected malware into the system that was successful in obtaining the login names and passwords of the highest executives at Equifax.

54. Using these credentials, the intruders were also able to exploit other services used by Equifax, such as Dropbox and LinkedIn.

55. After obtaining the stolen credentials on the Dark Web and reviewing them, Comodo found that Equifax's chief privacy officer, chief information officer, vice president of public relations, and vice president of sales used passwords with major security deficiencies such as all lowercase letters, no special symbols, and easily guessable words like spouses' names, city names, and even combinations of initials and birth years.

Equifax Refuses to Disclose the Fraudulent Procurement of Consumer Files

56. Despite knowing about the breach in July, Equifax kept the information secret. It did not reveal to individual consumers to whom it owed a contractual duty under a credit monitoring service. And it did not reveal to the public—those whose information was stolen and who stand to be injured from the breach—that the breach took place until September 8, 2017. But even then, Equifax has not disclosed exactly who was affected and what information was accessed.

57. The credit report information fraudulently procured from Equifax is all that is necessary to fraudulently obtain credit, tax returns and even a driver's license. With this information, an identity thief can now open credit, obtain full credit files from other CRAs, and even verify the falsified identity in future transactions.

58. Plaintiff and Class Members will incur costs associated with time spent and the loss of productivity from addressing and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance

of dealing with all issues resulting from the Data Breach; as well as damages to and diminution in value of their personal and financial information entrusted to Equifax.

59. And Equifax knows this, as well as the urgency of providing detailed information to victim consumers as soon as possible. It warns on its marketing site, "More than ever before, your employees and customers are at great risk for identity theft and fraud. Over 165 million data records of U.S. residents have been exposed due to data breaches since January 2005 - Privacy Rights Clearinghouse."[5]

60. Defendants (now ironically) boast of how effective and robust its data breach response time and program is, stating, "You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events every day. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market." *Id*. Such "industry leading" services and capabilities would, by Equifax's suggestion require the breached business to, "Quickly inform consumers[.]" *Id*.

61. Equifax has, however, not "quickly informed consumers" as to its own data breach. As of the date of this filing, Equifax still refused to substantively inform affected consumers. And Equifax waited at least six weeks before it publicly disclosed even the general fact of the data breach.

62. Customers who called the dedicated call center set up by Equifax were often unable to get a coherent or timely response.

63. Even the "free" credit monitoring it offered to hack victims came with a string. The Terms of Service for TrustedID (an Equifax owned company) contain a provision that an

[5] http://www.equifax.com/help/data-breach-solutions/ (last visited September 21, 2017).

individual's "membership subscription may be subject to automatic renewal."[6] Offering credit monitoring to every American through TrustedID also positions Equifax to collect even more valuable PII. To sign up, a consumer must authorize TrustedID to retrieve information about the consumer from the other two credit bureaus (Equifax and TransUnion). The information on the credit reports of the bureaus can vary by up to 20%, meaning Equifax can gain access to, and ultimately profit from, additional information from the other two credit bureaus when consumers grant TrustedID access to their Equifax and TransUnion credit files.

64. The system Defendants implemented to update consumers about whether their credit reporting information had been procured by the identity thieves was ineffective and not helpful. To take advantage of this look up, all you need to do is provide your last name and last six (not 4) digits of your Social Security number. However, the website that Equifax launched often returned the same message to a user regardless of what information was put in. [7] And, the site is not hosted on the Equifax network and appears to be a website domain and structure that was previously recognized as critically vulnerable to a hack. Since trust is critical for web sites like this, especially after a breach of this severity, it is difficult for consumers to trust that Equifax latest online support option is properly protecting their data.

65. Regardless, even assuming the Class Members did not suffer a false positive; Equifax has still refused to provide any detailed information as to what specific data was procured for individual consumers. And the generalized summary of the fact that they produced data including personal identifying information and some credit card account numbers is of little comfort to Plaintiff and Class Members. What specific documents or files were procured

6 https://www.trustedid.com/serviceterms.php?serviceterms (last visited Sept. 21, 2017).
7 https://www.riskbasedsecurity.com/2017/09/equifd-equifax-breach-response-off-to-a-rough-start/ (last visited September 21, 2017).

containing such information? What additional parts of the credit report file was obtained? Which database(s) were hacked and thus procured? What information does Equifax have as to who procured it?

66. Because of Equifax's breach of its duty of care to Plaintiff and Class Members, they suffered harm in that their personal information has been disseminated to criminals without their authorization, causing them stress, sleeplessness, headaches, and the like over the inability to know what has happened to their information or even what information has been accessed.

67. Plaintiff and Class Members also suffered out of pocket costs of at least $10 per security freeze they instituted because of the breach.

68. These individuals will incur subsequent costs with future transactions—they must pay to temporarily lift the security freeze to, for example, purchase a car, then pay to have it reinstated. They must also pay to have the freeze permanently lifted.

69. Plaintiff and Class Members also suffered the risk of harm in that the information that Equifax allowed to be taken may allow criminals to illegally access accounts belonging to Plaintiff and Class Members, to open accounts in Plaintiff's and Class Members' names without their authorization, and ruin Plaintiff's and Class Members' credit reputations by failing to pay debts they created using Plaintiff's and Class Members' personal information.

COUNT I: NEGLIGENCE
Class Claim

70. Plaintiff restates each of the allegations in the preceding paragraphs as if set forth at length herein.

71. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action for himself and on behalf of a class (the "Texas Class") defined as:

> All natural persons residing in the State of Texas whose personally identifiable information or financial information was breached as a result of the data breach announced by Equifax on or about September 7, 2017.

72. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action for himself and on behalf of a subclass (the "Security Freeze Subclass") defined as:

> All natural persons residing in the State of Texas whose personally identifiable information or financial information was breached as a result of the data breach announced by Equifax on or about September 7, 2017, and who paid a fee to Experian or TransUnion to institute a security freeze as that term is explained in Texas Business and Commerce Code Section 20.034.

73. Equifax's conduct in failing to protect Class Members' information, as described above, constitutes negligence. Equifax had a duty to act as would a reasonable CRA to safeguard the personal financial information of consumers entrusted to it by federal and state statutes.

74. Equifax breached that duty by failing to secure its systems, including but not limited to, applying a simple security patch that had been released for months prior to the break-in, then failing for months to notify Class Members that their information was compromised. As a proximate result of this breach of duty, Texas Class and Security Freeze Subclass Members suffered injuries. Those injuries resulted in monetary damages to Plaintiff and Class Members.

75. **Numerosity. FED. R. CIV. P. 23(a)(1).** Plaintiff is a member of the Class and Subclass. Plaintiff alleges that the members of the Class and each Subclass are so numerous that joinder of the claims of all class members is impractical. Plaintiff estimates that the Class and each Subclass are comprised of tens of thousands of consumers, likely exceeding 100,000 such individuals. Equifax operates as a national consumer-reporting agency and, upon information and belief, allowed illegal access to the personal information of millions of American consumers. The names and addresses of the Class Members are identifiable through documents maintained by

Equifax, Experian, and TransUnion, and the Class Members may be notified of the pendency of this action by published and/or mailed notice.

76. **Existence and Predominance of Common Questions of Law and Fact. Fed. R. Civ. P. 23(a)(2).** There are questions of law and fact common to the class, which common issues predominate over any issues involving only individual class members. For example, and without limitation, the focus of the litigation will be: (a) whether Equifax owed a duty of care to Class and Subclass Members; (b) whether it breached that duty; (c) whether the breach proximately harmed Class and Subclass Members; (d) whether Equifax's conduct caused damages to Class and Subclass Members'; (e) whether Equifax's credit monitoring products worked as advertised or represented; and (f) the appropriate amount of damages that are appropriate for such violations.

77. **Typicality. Fed. R. Civ. P. 23(a)(3)**. Plaintiff's claims are typical of those of the Class Members. All are based on the same facts and legal theories. Equifax uses common practices and automated systems in committing the conduct that Plaintiff alleges injured him and the Classes. Equifax's failure to adequately safeguard Class and Subclass Members' personal information was uniform across Class Members, as was the method by which this information was illegally accessed. Moreover, Equifax's representations regarding the robustness of its credit monitoring products was the same across Class and Subclass Members, so a claim for one Class Member is the same as the claim for another. Plaintiff seeks actual, statutory, and punitive damages for the Class and Subclass claims and, in addition, Plaintiff is entitled to relief under the same causes of action as the other members of the Class and each Subclass. The violations alleged are the same and the Class claims will rise or fall entirely based upon whether or not Plaintiff's claims rise or fall.

78. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiff will fairly and adequately protect the interests of the Class and Subclasses. Plaintiff's interests coincide with and are not antagonistic to the Class Members' interests. Plaintiff has retained counsel experienced in handling actions involving unlawful practices against consumers and class actions. Neither Plaintiff nor his Counsel has any interests that might cause them not to vigorously pursue this action. Plaintiff is aware of his responsibilities to the putative Classes and has accepted such responsibilities.

79. **Superiority. Fed. R. Civ. P. 23(b)(3).** Questions of law and fact common to the Class and Subclass Members predominate over questions affecting only individual members, and a class action is superior to other available methods for fair and efficient adjudication of the controversy. The damages sought by each member are such that individual prosecution would prove burdensome and expensive given the complex and extensive litigation necessitated by Equifax's conduct. It would be virtually impossible for the members of the Class and Subclass to individually redress effectively the wrongs done to them. Even if the members of the Class and Subclass themselves could afford such individual litigation, it would be an unnecessary burden on the courts. Furthermore, individualized litigation presents a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues raised by Equifax's conduct. By contrast, the class action device will result in substantial benefits to the litigants and the Court by allowing the Court to resolve numerous individual claims based upon a single set of proof in just one case.

80. Further, the Court is able to certify a liability-only class pursuant to Fed. R. Civ. P. 23(c)(4).

81. **Injunctive Relief Appropriate for the Class. Fed. R. Civ. P. 23(b)(2).** Certification of a class under Rule 23(b)(1) of the Federal Rules of Civil Procedure is proper.

Prosecuting separate actions by or against individual Class Members would create a risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

82. Certification of a class under Rule 23(b)(2) of the Federal Rules of Civil Procedure is appropriate in that Equifax has acted on grounds generally applicable to the class thereby making appropriate declaratory relief with respect to the class as a whole.

83. Certification of the class under Rule 23(b)(3) of the Federal Rules of Civil Procedure is also appropriate in that:

a. As alleged above, the questions of law or fact common to the members of the Class and Subclass predominate over any questions affecting an individual member. Each of the common facts and legal questions in the case overwhelm the more modest individual damages issues. Further, those individual issues that do exist can be effectively streamlined and resolved in a manner that minimizes the individual complexities and differences in proof in the case.

b. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Consumer claims generally are ideal for class treatment as they involve many, if not most, consumers who are otherwise disempowered and unable to afford and bring such claims individually. Further, most consumers affected by Equifax's negligence would likely be unaware of their rights under the law, or of whom could represent them in federal litigation. Additionally, individual litigation of the uniform issues in this case would be a waste of judicial resources as it increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues raised by Equifax's conduct. By contrast, the class action device will result in substantial benefits to the litigants and the Court by allowing the

Court to resolve numerous individual claims based upon a single set of proof in just one case. The issues at the core of this case are class wide and should be resolved at one time.

84. Plaintiff and other members of the Class and Subclass are entitled to recover their actual damages caused by Equifax's breach. They are also entitled to injunctive relief to prevent such further harm in the future.

85. As a result of these violations, Equifax is liable, to Plaintiff and each Class and Subclass Member for actual damages suffered as a result of Equifax's negligence.

WHEREFORE, Plaintiff requests the following relief:

A. That an order be entered certifying the proposed Texas Class and Security Freeze Subclass under Rule 23 of the Federal Rules of Civil Procedure and appointing Plaintiff Parkhill and his counsel to represent the Class and Subclass;

B. That judgment be entered for the Texas Class and Security Freeze Subclass against Defendant Equifax for damages, costs, and interest as may be allowed by law for its negligence; and

C. That the Court grant such other and further relief as may be just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff demands trial by jury as to all issues against Defendant Equifax.

/s/ Craig C. Marchiando
Craig C. Marchiando, SBT #24046347
Leonard A. Bennett (*pro hac vice forthcoming*)
Elizabeth Hanes (*pro hac vice forthcoming*)
CONSUMER LITIGATION ASSOCIATES, P.C.
763 J. Clyde Morris Blvd., Suite 1-A
Newport News, VA 23601
Telephone – (757) 930-3660
Fax – (757) 930-3662
Email: craig@clalegal.com
Email: lenbennett@clalegal.com
Email: elizabeth@clalegal.com